




STATE OF WASHINGTON

**MILITARY DEPARTMENT**

*Camp Murray • Tacoma, Washington 98430-5000*

**DIRECTIVE**

**To: All Military Department State Employees, Managers, and Supervisors**  
**From: Major General Timothy J. Lowenberg**   
**Subject: Agency Computing and Network Environment – Policy Notification – Acknowledgement of Receipt**  
**Date: March 23, 2012**

It is important that all Military Department staff follow and uphold agency policy as it relates to personal use and management of agency computers and networks. ***By this Directive I am requiring all Military Department state employees to read this Directive and Policy IT-306-05 and Information Technology Security Audits Procedure No. 001-12 and print and sign this Directive, and immediately submit to their supervisor for submission to the Human Resources Office.***

Attached to this Directive you will find a copy of the updated and revised agency policy IT-306-05, "Use of the Internet, Electronic Mail and Computer Systems". Personal files, documents, downloads, or any other materials that are not work related should not be stored on or transferred to agency owned computers, networks, or devices. The Information Technology Division will be performing recurring random audits of not less than 10-15% of all workstations at any one time at least once per quarter and may also perform individual and larger scale audits as directed by The Adjutant General. Employees who are found to be in non-compliance with Agency Policy will be subject to disciplinary action which may include dismissal from state employment. The following is a nonexclusive list of items, uses, and/or purposes for which agency owned computers, devices, telephones, networks, or access to the wired or wireless Internet that is not acceptable in any form. Please be advised, the below list is not all inclusive. If you are in doubt it is best to ask BEFORE you make the decision to:

- Download, transfer, or store MP3, music or streaming video files that are not directly related to your work
- Download or install any unauthorized software, media players, programs, or files that are not authorized in accordance with IT policy
- Download, send, transfer, watch, or store personal videos, jokes, etc.
- Download, send, transfer or store an excessive amount of personal pictures
- Use of agency owned wired or wireless Internet to listen to the radio, watch movies or television shows, podcasts, or access YouTube or other similar sites for purposes that are not directly related to your work
- Use of agency owned computers or devices to store, print, transfer, or work on individual course study (homework) from any class not sanctioned by the Military Department with express permission to complete during work hours
- Processing of any personal documents to include, but not limited to, mortgages, loans, bank statements, income taxes, adoption paperwork, health care claims, credit applications, credit reports, bankruptcy filings, insurance applications, child care custodial or care plans, etc.
- Use of agency owned devices or agency owned wired or wireless Internet to check personal email, Facebook, Twitter, or LinkedIn accounts; check bank balances, pay bills, play games, search for real estate, shop, make personal travel arrangements or surf for items of a personal nature at any time during work or non-work hours
- Use of agency owned software, including but not limited to Microsoft Excel, OneNote, Outlook, PowerPoint, Publisher, Word, etc., to create documents that are personal in nature such as

personal budgets, calendars, party invitations, job applications for self, friends or family members, children's homework, etc.

- Unapproved devices may not be connected to or backed up on state computers or networks; i.e., cell phones, personal hard drives, MP3 players, etc.
- Unapproved devices (which include but are not limited to personal cell phones, thumb drives, external hard drives, memory cards, etc.) may not be utilized to store agency owned information or data
- Perform any outside work activities (this includes use of all other agency owned equipment as well) at any time during work or non-work hours
- Perform any political or campaign activities on agency owned devices or agency owned wired or wireless networks at any time during work or non-work hours

If you have questions about the appropriateness of the use of agency owned computing and technology resources, the agency network or the wired or wireless Internet, contact Mark Glenn, Chief Information Security Officer, Information Technology; or Laura Drybread, Human Resources Director and Agency Ethics Advisor.

***Acknowledgment of Receipt:***

***I acknowledge that I have received a copy of this Directive and Policy IT-306-05. I have read this Directive and Policy No. IT-306-05, understand that I am responsible for complying with the provisions of Policy IT-306-05, and further acknowledge that a signed copy of this Directive is being placed in my official personnel file.***

\_\_\_\_\_  
Employee Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor Signature

\_\_\_\_\_  
Date